



Verizon Wireless
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005

Phone 202 589-3740
Fax 202 589-3750

February 27, 2009

VIA ECFS

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th St., SW
Suite TW-A235
Washington, DC 20554

Re: *Annual CPNI Certification, EB Docket No. 06-36*

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. § 64.2009(e), Alltel Communications, LLC (Alltel), hereby files its annual certification of compliance with the Commission's customer proprietary network information (CPNI) rules. Attached to the certification is a list of companies covered by Alltel's certification. As a result of a merger that was consummated on January 9, 2009, Alltel became a wholly-owned subsidiary of Cellco Partnership d/b/a Verizon Wireless.

Please contact the undersigned at (202) 589-3770 should you have any questions.

Sincerely,

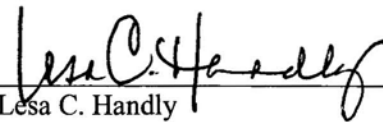
A handwritten signature in cursive script, appearing to read "Tamara L. Preiss".

Tamara L. Preiss

cc: Best Copy and Printing, Inc. (via e-mail)

**ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION**

I, Lesa C. Handly, was a duly authorized officer of Alltel Communications, LLC ("Alltel") for the year 2008 and am currently an employee of Verizon Wireless as a result of the Verizon Wireless - Alltel merger that was consummated on January 9, 2009. In that capacity, I hereby certify on behalf of Alltel that I have personal knowledge that during the period from January 1, 2008 through January 9, 2009, Alltel had operating procedures, as described in sections A through C of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.



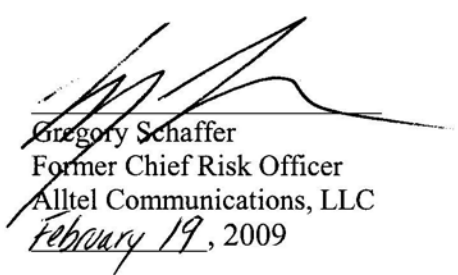
Lesla C. Handly

Former Senior Vice President – Customer Strategies
Alltel Communications, LLC

FEBRUARY 26, 2009

ALLTEL COMMUNICATIONS, LLC
ANNUAL SECTION 64.2009(e) CERTIFICATION

I, Gregory Schaffer, was a duly authorized officer of Alltel Communications, LLC ("Alltel"), for the year 2008 and am currently an employee of Verizon Wireless as a result of the Verizon Wireless - Alltel merger that was consummated on January 9, 2009. In that capacity, I hereby certify on behalf of Alltel that I have personal knowledge that during the period from January 1, 2008 through January 9, 2009, Alltel had operating procedures, as described in sections D through J of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), that, to the best of my knowledge, information and belief, were adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.

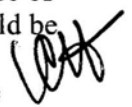


Gregory Schaffer
Former Chief Risk Officer
Alltel Communications, LLC
February 19, 2009

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING
47 C.F.R. SUBPART U GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION
FOR THE PERIOD JANUARY 1, 2008 TO JANUARY 9, 2009**

The following explains how the operating procedures of Alltel Communications, LLC ("Alltel") ensured that it was in compliance with the Commission's CPNI rules, as referenced herein and set forth in 47 C.F.R. Subpart U. On January 9, 2009, Alltel merged with and became a wholly owned subsidiary of Cellco Partnership d/b/a Verizon Wireless.


A. CPNI Use and Customer Approval

In accordance with 47 CFR 64.2005(a), Alltel used CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribed from Alltel. During the relevant time period, Alltel offered CMRS and information services. Consistent with 47 CFR 64.2005(b), Alltel did not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribed. Alltel used CPNI derived from the provision of CMRS for the provision of CPE and information services. Alltel did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and Alltel did not consider its customers' to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers did not apply to Alltel's operational use of CPNI in 2008. Alltel maintained a CPNI Marketing Policy which defined how CPNI could be used to market and provide services to Alltel customers. In accordance with that policy, Alltel required that CPNI be used only for the purposes identified herein and as otherwise permitted. 

B. Sales and Marketing Campaigns


Pursuant to 47 CFR 64.2009, Alltel reviewed sales and marketing campaigns that used CPNI. All such campaigns were conducted to market services within the category of service to which the customer subscribed from Alltel in accordance with 47 CFR 64.2005(a). Alltel did not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Alltel had a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Alltel restricted the ability to create marketing campaigns in order to ensure compliance with the CPNI rules. The persons with authority to approve campaigns which used CPNI were at minimum Director level employees.

Consistent with 47 CFR 64.2009(c), Alltel maintained records of the campaigns which used CPNI that were conducted by authorized personnel. Alltel's Privacy Office conducted quarterly reviews of such campaign records to verify compliance with CPNI rules and Alltel policies. These records contain a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of


the campaign. This information is retained for at least one year. The results of the quarterly reviews were also analyzed by the Privacy Office and Legal staff to verify compliance with CPNI rules. 

C. Training and Disciplinary Process


Alltel employees authorized to conduct marketing campaigns were trained to keep customer data strictly confidential. Alltel's Privacy Office conducted periodic CPNI education for personnel who were authorized to conduct campaigns as required by 47 CFR 64.2009(b). Specifically, such personnel were instructed as to the proper access and use of CPNI. Each person authorized to conduct a marketing campaign utilizing CPNI received this education.


Alltel's CPNI Marketing Policy expressly established a disciplinary process applicable to employees in the event it was determined that such policy had been violated. A violation of such policy would subject the employee to disciplinary action, up to and including termination. 

D. Security Governance


Alltel established an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by the Company. Pursuant to the EISP, Alltel maintained a Security Steering Committee that included (among others) the Chief Operating Officer, the General Counsel, the Chief Financial Officer, the Executive Vice President for Network Services and the Senior Vice Presidents of Human Resources and IT Services. Alltel's Chief Security and Risk Officer was responsible for an Enterprise Security and Risk Office that developed, implemented and enforced security and privacy policies on a company wide basis. 

E. Billing Records, Network Records, and Information

Alltel maintained billing detail data, call detail data, and network record data in applications secured by networks, systems, policies and processes designed to control, monitor, and limit access to authorized users with legitimate business needs. 

Internal governance processes dictated that newly created applications and significant changes to existing applications that processed or stored customer data must be formally reviewed and analyzed by appropriate security and privacy teams. Alltel's Enterprise Security and Risk team reviewed new applications and enhancements for compliance with existing security and privacy policies, which included requirements for access and authentication controls. Alltel's Internal Audit Department routinely reviewed applications to test for compliance with then existing security procedures. 

F. Data Centers

All data centers had processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security 

policies was reviewed by the Enterprise Security and Risk team and Internal Audit on a recurring basis.

G. Safeguards on the Disclosure of CPNI

(1) Safeguarding CPNI

Alltel's account verification policy established the circumstances and limitations under which Alltel call center and retail employees were allowed to disclose CPNI. These employees were monitored and rated for compliance with Alltel's account verification procedures.

Alltel employees were trained to keep sensitive customer data strictly confidential and suspected breaches of customer confidentiality were investigated by corporate security teams. In addition to investigating reported incidents, security teams periodically conducted reviews of various systems to identify potential unauthorized access to customer data. Alltel required newly-hired employees to sign an "Employee Agreement on Non-Disclosure and Non-Solicitation," which prohibited employees from disclosing information that was confidential to any third party. Confirmed unauthorized disclosures of customer information were subject to discipline, up to and including termination and referrals to law enforcement authorities where deemed appropriate.

Policies, practices and technologies were used to limit employee access to customer records on a business need basis. Initial access to a number of applications was controlled via an internal application that used role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function. Access to relevant financial reporting applications were reviewed quarterly by the designated business owner for Sarbanes-Oxley compliance. Quarterly reviews were also conducted of certain other applications containing sensitive customer or company data.

Alltel's privacy statement described how Alltel used, maintained and protected customer information, including CPNI. During 2008 this statement was available to all customers at www.alltel.com by clicking on 'Privacy Statement' at the bottom of Alltel's home page. In addition, Alltel's contracts with independent contractors that had access to confidential customer data were required to contain safeguards necessary to protect that data.

(2) Telephone Access to CPNI

By policy, reinforced with training and monitoring, Alltel customer service representatives were prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone. A customer service representative was allowed to assist the customer in the event an authenticated customer first identified the call to the representative without assistance during a call initiated by the customer. Upon request, Alltel would mail a copy of call detail to the customer's address of record. In the event a customer's address of record had changed in the thirty days prior to the telephone request, Alltel did not mail the requested call detail. Instead, Alltel advised such customers to utilize online or in-store access. Alltel policy did not permit faxing of call detail.

(3) Online Access to CPNI

Alltel maintained an online account retrieval system called "My Account" whereby Alltel customers could register their account and subsequently login to access their account information and CPNI only after providing a valid password. Prior to the relevant time period, Alltel had established operating procedures adequate to ensure compliance with the newly enacted CPNI rules relating to online access to CPNI, including a requirement that all customers who register for My Account receive a text message to the designated handset on the account being registered. Pursuant to these procedures, a code in the text message would be required to complete the registration process. All of the established procedures described herein were fully implemented prior to the relevant time period except the registration text message delivery to post paid customers, which was fully implemented on February 17, 2008.

Alltel customers who wanted online access to their account information and CPNI first needed to register their account on My Account. Prior to beginning the registration process, customers were required to provide Alltel their account number and mobile number. The post paid registration process required customers to: (1) provide their name; (2) create a unique user identification; (3) create a password; and (4) provide their electronic mail address.

My Account registration for Alltel business customers required two data elements in addition to the My Account registration process for post paid consumers. Business customers were required to provide their business' tax identification number to Alltel and to create a personal identification number (PIN) after they entered their user identification and password. For on-line access to CPNI after the registration for a business account was complete, users were required to submit their user identification, password and PIN.

Alltel prepaid customers registered for online access to CPNI in the same manner as described above. Prepaid customers were sent a text message containing a unique code to their handset which was then used to complete the My Account registration process. Thereafter, prepaid customers were required to utilize their user identification and password for online access to CPNI.

Additionally, Alltel provided all customers the ability to block online access to their account and CPNI.

(4) Establishment of a Password and Back-Up Authentication Methods for Lost or Forgotten Passwords.

Alltel made available a backup authentication method for customers who had forgotten their My Account password. This backup authentication method did not prompt the customer for readily available biographical or account information. If the customer did not provide the correct response for the backup authentication method, the customer was sent a code via text message to their handset. The customer was required to provide this code to Alltel prior to establishing a new password.

(5) Notification of Account Changes

Alltel immediately notified customers via text message to their handset or United States mail to their address of record, when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record was created or changed. Alltel did not reveal the changed information.



(6) In-Store Access to CPNI

Alltel required customers to present valid photo identification and verified the identity matched the account information prior to disclosing CPNI at an Alltel retail location and at Alltel agent retail locations.



H. Notification of CPNI Security Breaches

Alltel enhanced existing processes in order to comply with the CPNI rules. Regular recurring meetings were conducted among Alltel's Enterprise Security and Risk Office and Legal staff to consider internal investigations involving potential CPNI breaches. Alltel reported confirmed CPNI breaches and notified customers in accordance with the CPNI breach notification rules.



I. Summary of Customer Complaints Regarding the Unauthorized Release of CPNI

During the relevant period Alltel received 72 complaints from customers regarding the unauthorized release of CPNI. Alltel's Enterprise Security and Risk Office investigated these complaints and 41 of them did not appear to result in improper access to or unauthorized release of CPNI. There were 23 instances of apparent improper access and improper disclosure by employees to unauthorized individuals, 3 instances of handsets containing customer information being released through theft or process violations, 4 instances of potential online breaches, and 1 instance of Authorized Agent misconduct.



J. Action Taken Against Data Brokers

During the relevant period, Alltel did not initiate any actions against data brokers in 2008.



Alltel-Affiliated Licensees (Form 499A Filer ID)

ALLTEL Communications, LLC (823790)
ALLTEL Central Arkansas Cellular Limited Partnership (806208)
ALLTEL Communications of Arkansas RSA 12 Cellular Limited Partnership (806033)
ALLTEL Communications of LaCrosse Limited Partnership (806033)
ALLTEL Communications of North Carolina Limited Partnership (818374)
ALLTEL Communications of Saginaw MSA Limited Partnership (806033)
ALLTEL Northern Arkansas RSA Limited Partnership (806205)
Arkansas RSA #2 (Searcy County) Cellular Limited Partnership (818074)
Celutel of Biloxi, Inc. (806033)
Charleston-North Charleston MSA Limited Partnership (818424)
Fayetteville MSA Limited Partnership (806222)
Georgia R.S.A. #8 Partnership (806211)
Jackson Cellular Telephone Co., Inc. (806033)
Las Cruces Cellular Telephone Company (820115)
Michigan RSA #9 Limited Partnership (806033)
Missouri RSA #15 Limited Partnership (806238)
Missouri RSA 2 Partnership (806226)
Missouri RSA 4 Partnership (806232)
Northwest Arkansas RSA Limited Partnership (806254)
Ohio RSA #3 Limited Partnership (807579)
Ohio RSA 2 Limited Partnership (818484)
Ohio RSA 5 Limited Partnership (818486)
Ohio RSA 6 Limited Partnership (818488)
Oklahoma RSA No. 4 South Partnership (806227)
Pascagoula Cellular Partnership (806033)
Petersburg Cellular Partnership (818432)
Texas RSA #11B Limited Partnership (818450)
Texas RSA 7B2 Limited Partnership (818442)
Tyler/Longview/Marshall MSA Limited Partnership (818402)
Virginia RSA 2 Limited Partnership (818492)
Wisconsin RSA #1 Limited Partnership (806033)
Wisconsin RSA #2 Partnership (806033)
Wisconsin RSA #6 Partnership, LLP (806033)
Wisconsin RSA No. 7 Partnership (806033)
Wisconsin RSA No. 8 Limited Partnership (806033)